

(19)

JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: **11041231 A**

(43) Date of publication of application: **12.02.99**

(51) Int. Cl

H04L 9/32
G09C 1/00
G09C 1/00
H04L 9/08

(21) Application number: 09208447

(22) Date of filing: 17.07.97

(71) Applicant: **NIPPON TELEGR & TELEPH
CORP <NTT>**

(72) Inventor: **TAKADA SHUNSUKE
NAKAMURA TAKAO
OGAWA HIROSHI
KAWAKUBO HIDEJI**

(54) ORIGINAL INFORMATION PROTECTION
METHOD AND DEVICE FOR INFORMATION
DISTRIBUTION SYSTEM

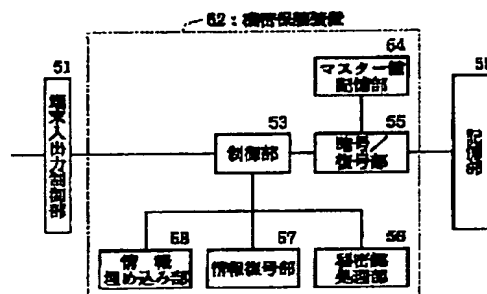
(57) Abstract:

PROBLEM TO BE SOLVED: To prevent a user from copying illicitly the original information based on the purchased encipherment information by using an external device to decode the enciphered distributed information, to embed a user authenticator into the decoded original information and also to manage the keys which are used for both decoding and embedding processes.

SOLUTION: This original information protection device (external device) 50 consists mainly of an information decoding part 57 and an information embedding part 58. When the device 50 is produced, a master key that is inherent to the device 50 is stored in a master key storage part 54 of a security device 52. At an enciphering/decoding part 55, a user's secret key is enciphered by the master key that is stored in the part 54 and this enciphered key is stored in a storage part 59. The control part of a user terminal receives the enciphered key via an open key and sends this received key to the device 50. A terminal input/output control part 51 of the device 50 sends the received key to a control part 53.

COPYRIGHT: (C)1999,JPO

60: 原情報保護装置 (外部装置)



Express Mail EL03979066705

(19)日本国特許庁(JP)

(12)公開特許公報 (A)

(11)特許出願公開番号

特開平 1 1 - 4 1 2 3 1

(43)公開日 平成11年(1999)2月12日

(51)Int. Cl.⁶
H 0 4 L 9/32
G 0 9 C 1/00
H 0 4 L 9/08

識別記号
6 4 0
6 6 0

F I
H 0 4 L 9/00 6 7 5 A
G 0 9 C 1/00 6 4 0 D
H 0 4 L 9/00 6 6 0 A
6 0 1 A
6 0 1 E

審査請求 未請求 請求項の数 7

F D

(全 9 頁) 最終頁に続く

(21)出願番号 特願平 9 - 2 0 8 4 4 7

(22)出願日 平成9年(1997)7月17日

(71)出願人 000004226

日本電信電話株式会社
東京都新宿区西新宿三丁目19番2号

(72)発明者 高田 俊介

東京都新宿区西新宿三丁目19番2号 日本
電信電話株式会社内

(72)発明者 中村 高雄

東京都新宿区西新宿三丁目19番2号 日本
電信電話株式会社内

(72)発明者 小川 宏

東京都新宿区西新宿三丁目19番2号 日本
電信電話株式会社内

(74)代理人 弁理士 川久保 新一

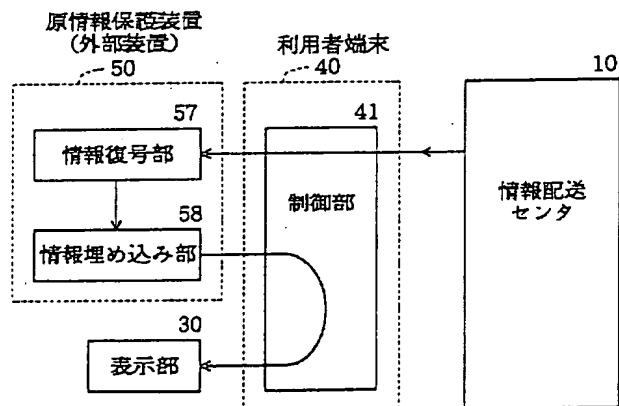
最終頁に続く

(54)【発明の名称】 情報流通システムにおける原情報保護方法およびその装置

(57)【要約】

【課題】 情報流通システムにおいて、利用者が購入した暗号化情報に基づいて、利用者が原情報を不正複製することを阻止することができる原情報保護方法およびその装置を提供することを目的とするものである。

【解決手段】 暗号化されている流通情報を復号する処理を利用者端末の外部装置で実行させ、また、復号した原情報に利用者認証子を埋め込む処理を上記外部装置で実行させ、さらに、上記復号処理と上記埋め込む処理とに使用する鍵を上記外部装置が管理するものである。



【特許請求の範囲】

【請求項 1】 情報流通システムにおいて、暗号化されている原情報を復号する原情報復号手段と；上記復号された原情報に、情報埋め込み鍵によって利用者認証子を埋め込む利用者認証子埋め込み手段と；を有し、上記原情報復号手段と、上記利用者認証子埋め込み手段とが、利用者端末の外部に設けられていることを特徴とする情報流通システムにおける原情報保護装置。

【請求項 2】 請求項 1 において、上記原情報復号の処理と上記利用者認証子埋め込みの処理とに使用する鍵を管理することを特徴とする情報流通システムにおける原情報保護装置。

【請求項 3】 請求項 1 において、公開鍵暗号方式の利用者公開鍵によって情報配送センタで暗号化された情報暗号鍵、情報埋め込み鍵、利用者認証子を、利用者秘密鍵によって復号する復号手段と；上記復号された情報暗号鍵、情報埋め込み鍵、利用者認証子を記憶する記憶手段と；を有することを特徴とする情報流通システムにおける原情報保護装置。

【請求項 4】 請求項 1 において、秘密鍵処理部と情報復号部と情報埋め込み部とを具備する機密保護装置を有し、上記秘密鍵処理部は、情報配送センタにおいて利用者の公開鍵で暗号化された情報暗号鍵、情報埋め込み鍵、利用者認証子を復号するものであり、上記情報復号部は、上記情報配送センタで暗号化された情報を、上記情報暗号鍵によって復号するものであり、上記情報埋め込み部は、上記利用者認証子を復号した情報に埋め込む装置であることを特徴とする情報流通システムにおける原情報保護装置。

【請求項 5】 情報流通システムにおいて、マスター鍵記憶部と暗号／復号部とを具備する機密保護装置と、記憶部とを有し、上記暗号／復号部は、上記記憶部に情報を送信するときに、上記マスター鍵記憶部に格納してあるマスター鍵で暗号化し、上記記憶部から情報を受信するときに復号する装置であることを特徴とする情報流通システムにおける原情報保護装置。

【請求項 6】 情報流通システムにおいて、暗号化されている原情報を復号する原情報復号段階と；上記復号された原情報に、情報埋め込み鍵によって利用者認証子を埋め込む利用者認証子埋め込み段階と；を有し、上記原情報復号段階と、上記利用者認証子埋め込み段階とが、利用者端末の外部で実行されることを特徴とする情報流通システムにおける原情報保護方法。

【請求項 7】 情報流通システムにおいて、暗号化されている原情報を復号する原情報復号手段と；上記復号された原情報に、情報埋め込み鍵によって利用者認証子を埋め込む利用者認証子埋め込み手段と；としてコンピュータを機能させるためのプログラムを記録し

たコンピュータ読取可能な記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、情報流通システムにおいて、原情報を保護する方法およびその装置に関する。

【0002】

【従来の技術】従来の情報流通システム I F S において、利用者が情報配送センタから流通情報を購入する場合、利用者が上記流通情報を不正に二次利用することを抑止するために、利用者が流通情報を購入し、この流通情報を復号した原情報に利用者認証子を埋め込む方式が採用されている。なお、上記不正の例としては、プログラムの改竄や、利用者端末または情報配送センタへの不正が考えられる。

【0003】図 4 は、従来の情報流通システム I F S を示すブロック図である。

【0004】図 5 は、上記従来例の動作を示す図である。

20 【0005】情報流通システム I F S において、情報配送センタ 1 0 で原情報が暗号化され、情報配送センタ 1 0 から利用者が暗号化された原情報を購入し、利用者端末 2 0 において、原情報が復号され、この復号された原情報が表示部 3 0 に表示される。なお、利用者端末 2 0 は、制御装置 2 1 を有し、この制御装置 2 1 は、暗号化された原情報を復号する復号部 2 2 と、復号された原情報に利用者認証子を埋め込む情報埋め込み部 2 3 とを有する。

30 【0006】上記のように、復号した原情報に利用者認証子を埋め込むようにすれば、その原情報を二次利用すると、その原情報に利用者認証子がついて回るので、利用者はその情報を二次利用することができない。

【0007】

【発明が解決しようとする課題】しかし、上記従来例において、利用者端末で利用者が不正することによって、利用者認証子が埋め込まれていない原情報を入手することが可能である。

40 【0008】つまり、従来の情報流通システムにおいて、暗号化された原情報を情報配送センタから利用者が購入した後、暗号化された原情報を復号鍵によって復号し、この復号された原情報に利用者認証子が埋め込まれるのに先立って、上記復号鍵や復号された原情報がメモリ上に一時的に展開される。ここで、この復号鍵や復号された原情報を抽出するプログラムや装置を、利用者が自分の利用者端末にしかけることが可能である。すなわち、暗号化された情報を復号化するプログラムや、復号化された原情報をハードディスク等に落すプログラムを利用者が作り、このようなプログラムを使用することによって、復号された原情報を利用者が入手することができ

【0009】また、復号用の鍵が利用者に盗まれた場合、利用者認証子が原情報に埋め込まれる前に、暗号化情報が原情報に復号され、この原情報が利用者に入手されるという問題がある。

【0010】この結果、復号された原情報が利用者によって不正に複製され、その利用者が、複製した原情報を再び流通させること等が可能になり、原情報の提供者の利益が損なわれるという問題がある。

【0011】本発明は、情報流通システムにおいて、利用者が購入した暗号化情報に基づいて、利用者が原情報を不正複製することを阻止することができる原情報保護方法およびその装置を提供することを目的とするものである。

【0012】

【課題を解決するための手段】本発明は、暗号化されている流通情報を復号する処理を利用者端末の外部装置で実行させ、また、復号した原情報に利用者認証子を埋め込む処理を上記外部装置で実行させ、さらに、上記復号処理と上記埋め込む処理とに使用する鍵を上記外部装置が管理するものである。

【0013】

【発明の実施の形態および実施例】図1は、本発明の一実施例である原情報保護装置（外部装置）50を、利用者端末40と情報配送センタ10とともに示すブロック図である。

【0014】原情報保護装置（外部装置）50は、主に、情報復号部57と、情報埋め込み部58とを有するものであり、ICカード、PCカード等の計算機用カード、またはボード等の形態を有するものである。

【0015】初期条件としては、次のようなものである。まず、情報配送センタ10は、公開鍵暗号方式の秘密鍵Kcsを持ち、公開鍵Kcpを公開している。利用者は、公開鍵暗号方式の秘密鍵Kusを持ち、公開鍵Kupを公開している。

【0016】外部装置50を製造するときに、機密保護装置52内のマスター鍵記憶部54に、装置固有のマスター鍵Kmを格納する。

【0017】マスター鍵記憶部54に記憶されているマスター鍵Kmによって、暗号／復号部55において、利用者の秘密鍵Kusが暗号化され、このマスター鍵Kmで暗号化された秘密鍵Km[Kus]が記憶部59に格納される。

【0018】また、情報配送センタ10は、流通情報Mを登録し、情報Mに対する暗号鍵Keと情報埋め込み鍵Kwとを生成し、暗号鍵Keによって情報Mにスクランブルを施し、暗号化情報Ke[M]を生成する。また、情報配送センタ10は、スクランブルが施された流通情報Ke[M]を流通させる。

【0019】一方、利用者端末40における制御部41は、スクランブルが施された流通情報Ke[M]を受信

し、この受信した流通情報Ke[M]を表示部30に表示し、スクランブルが施された流通情報Ke[M]を閲覧する。そして、流通情報Ke[M]を利用者が購入する場合、購入要求と、利用者認証子Uidと、パスワードPwとを、情報配送センタ10に送信する。

【0020】なお、上記処理の代わりに、次のように処理するようにしてもよい。つまり、まず、情報提供者は、情報Mと、情報Mを容易に想像することができるサイズが小さい情報M'（画像情報の場合はサイズを小さくした画像情報、プログラムやゲーム等の場合は体験版等）とを作成し、これら情報Mと、サイズが小さい情報M'とを情報配送センタ10に登録し、情報配送センタ10は、サイズが小さい情報M'を流通させる。そして、利用者から購入要求があると、情報配送センタ10は、暗号鍵Keと情報埋め込み鍵Kwとをランダムに生成し、情報Mを暗号鍵Keで暗号化し、この暗号鍵Keで暗号化された情報Ke[M]を生成する。その後、暗号鍵Ke、情報埋め込み鍵Kw、利用者認証子Uidを利用者の公開鍵で暗号化したものと、暗号化情報Ke[M]とを、利用者へ送信するようにしてもよい。

【0021】情報配送センタ10は、利用者認証子UidとパスワードPwとに基づいて利用者認証を行う。また、流通情報Mの暗号鍵Keと情報埋め込み鍵Kwと利用者認証子Uidとを、それぞれ、利用者の公開鍵Kupによって暗号化し、公開鍵Kupによって暗号化された暗号鍵Kup[Ke]、公開鍵Kupによって暗号化された情報埋め込み鍵Kup[Kw]、公開鍵Kupによって暗号化された利用者認証子Kup[Uid]を生成する。そして、これら生成された公開鍵Kupによって暗号化された暗号鍵Kup[Ke]、公開鍵Kupによって暗号化された情報埋め込み鍵Kup[Kw]、公開鍵Kupによって暗号化された利用者認証子Kup[Uid]を利用者端末40に送信する。

【0022】図2は、原情報保護装置50の具体例を示すブロック図である。

【0023】原情報保護装置（外部装置）50は、端末入出力制御部51と、機密保護装置52と、記憶部59とを有する。機密保護装置52は、制御部53と、マスター鍵記憶部54と、暗号／復号部55と、秘密鍵処理部56と、情報復号部57と、情報埋め込み部58とを有する。

【0024】次に、上記実施例における利用者側の動作について説明する。

【0025】図3は、上記実施例の動作を示すフローチャートである。

【0026】まず、利用者端末40の制御部41は、公開鍵Kupによって暗号化された暗号鍵Kup[Ke]を受信し、この暗号鍵Kup[Ke]を外部装置50に送信し、外部装置50の端末入出力制御部51は、上記暗号鍵Kup[Ke]を、制御部53に渡す。そして、

マスター鍵Kmで暗号化された秘密鍵Km [Kus] が記憶部59に格納されており、この格納されている秘密鍵Km [Kus] を、マスター鍵記憶部54に格納されているマスター鍵Kmによって暗号/復号部55が復号するように、制御部53が制御し、秘密鍵Kusが得られる。

【0027】また、公開鍵Kupによって暗号化された暗号鍵Km [Ke] を、利用者の秘密鍵Kusによって、秘密鍵処理部56が復号するように、制御部53が制御し、暗号鍵Keが得られる。マスター鍵Kmによって、暗号/復号部55が暗号鍵Keを暗号化し、この暗号化された暗号鍵Km [Ke] を記憶部59に格納するように、制御部53が制御する。また、暗号鍵Km [Ke] の格納場所を識別する識別子Ke-IDを、制御部53が、端末入出力制御部51から制御部41へ返す。

【0028】そして、公開鍵Kupによって暗号化された情報埋め込み鍵Kup [Kw]、公開鍵Kupによって暗号化された利用者認証子Kup [Uid] についても、上記処理と同様の処理を行い、マスター鍵Kmによって暗号化された情報埋め込み鍵Km [Kw]、マスター鍵Kmによって暗号化された利用者認証子Km [Uid] を、記憶部59に格納し、情報埋め込み鍵Km [Kw]、利用者認証子Km [Uid] の格納場所を識別する識別子Kw-ID、Uid-IDを、制御部53が、端末入出力制御部51から制御部41へ返す。

【0029】次に、利用者端末40の制御部41は、受信した暗号化情報Ke [M] と識別子Ke-IDとを外部装置50へ送信し、端末入出力制御部51は、暗号化情報Ke [M] を制御部53に渡す。

【0030】制御部53は、記憶部59に格納されている暗号鍵Km [Ke] を、識別子Ke-IDに基づいて抽出し、暗号/復号部55が、この抽出された暗号鍵Km [Ke] をマスター鍵Kmで復号し、暗号鍵Keを得る。暗号鍵Keによって暗号化情報Ke [M] を情報復号部57が復号し、情報Mを得るように制御部53が制御する。また、マスター鍵Kmによって情報Mを暗号/復号部55が暗号化し、記憶部59に格納し、暗号化情報Km [M] を得るように、制御部53が制御する。

【0031】そして、制御部53は、暗号化情報Km [M] の格納場所を識別する識別子M-IDを、端末入出力制御部51から制御部41へ返す。制御部41は、識別子M-ID、Kw-ID、Uid-IDを外部装置50へ送信し、端末入出力制御部51は、上記情報を制御部53に渡す。記憶部59に格納された暗号化鍵Km [Kw]、暗号化利用者認証子Km [Uid]、記憶部59に格納された暗号化情報Km [M] を、識別子Kw-ID、Uid-ID、M-IDによって抽出し、暗号/復号部55がマスター鍵Kmで復号し、鍵Kw、利用者認証子Uid、情報Mを得るように、制御部53が制御する。

【0032】また、情報埋め込み部58が、鍵Kwによって情報Mに利用者認証子Uidを埋め込み、利用者認証子Uidが埋め込まれた情報Kw [M] を生成するように、制御部53が制御する。端末入出力制御部51から、利用者認証子Uidが埋め込まれた情報Kw [M] を制御部41に返すように、制御部53が制御し、外部装置50から返却された利用者認証子Uid埋め込み情報Kw [M] を表示部30が表示するように、制御部41が制御する。

【0033】なお、端末入出力制御部51から利用者認証子Uid埋め込み情報Kw [M] を制御部41に返し、外部装置50から返却された利用者認証子Uid埋め込み情報Kw [M] を表示部30が表示する代わりに、次のように処理してもよい。つまり、暗号/復号部55が、利用者認証子Uidが埋め込まれた情報Kw [M] をマスター鍵Kmによって暗号化し、暗号化情報Km [Kw [M]] を生成し、記憶部59に格納し、格納場所を識別する識別子Kw [M] -IDを、制御部41に返すように、制御部53が制御し、制御部41から、識別子Kw [M] -IDと表示命令とを受信したときに、識別子Kw [M] -IDによって、記憶部59から暗号化情報Km [Kw [M]] を抽出し、暗号化情報Km [Kw [M]] を暗号/復号部55がマスター鍵Kmで復号し、利用者認証子Uidが埋め込まれた情報Kw [M] を生成し、端末入出力制御部51から制御部41へ返すように処理するようにしてもよい。

【0034】また、上記実施例において、情報流通システムにおいて、暗号化されている原情報を復号する原情報復号手段と、復号された原情報に、情報埋め込み鍵によって利用者認証子を埋め込む利用者認証子埋め込み手段とを有し、上記原情報復号手段と上記利用者認証子埋め込み手段とが、利用者端末の外部に設けられていれば、情報流通において利用者が購入した情報から原情報を抽出することを防止することができる。

【0035】この場合、原情報復号の処理と利用者認証子埋め込みの処理とに使用する鍵を原情報保護装置が管理するようにすれば、利用者による原情報抽出を確実に防止することができる。

【0036】また、公開鍵暗号方式の利用者公開鍵によって情報配送センタで暗号化した情報暗号鍵、情報埋め込み鍵、利用者認証子を、利用者秘密鍵によって復号する復号手段と、上記復号された情報暗号鍵、情報埋め込み鍵、利用者認証子を記憶する記憶手段とを原情報保護装置に持たせれば、利用者による原情報抽出をより確実に防止することができる。

【0037】さらに、秘密鍵処理部と情報復号部と情報埋め込み部とを具備する機密保護装置を有し、上記秘密鍵処理部は、情報配送センタにおいて利用者の公開鍵で暗号化された情報暗号鍵、情報埋め込み鍵、利用者認証子を復号するものであり、上記情報復号部は、上記情報

配送センタで暗号化された情報を、上記情報暗号鍵によって復号するものであり、上記情報埋め込み部は、上記利用者認証子を復号した情報に埋め込む装置であるようにすれば、利用者による原情報抽出をさらに確実に防止することができる。

【0038】また、マスター鍵記憶部と暗号／復号部とを具備する機密保護装置と、記憶部とを有し、上記暗号／復号部は、上記記憶部に情報を送信するときに、上記マスター鍵記憶部に格納してあるマスター鍵で暗号化し、上記記憶部から情報を受信するときに復号する装置

であるようにすれば、利用者による原情報抽出をより一層確実に防止することができる。

【0039】なお、上記実施例を方法の発明として把握することができる。つまり、上記実施例は、情報流通システムにおいて、暗号化されている原情報を復号する原情報復号段階と、上記復号された原情報に、情報埋め込み鍵によって利用者認証子を埋め込む利用者認証子埋め込み段階とを有し、上記原情報復号段階と、上記利用者認証子埋め込み段階とが、利用者端末の外部で実行される情報流通システムにおける原情報保護方法である。

【0040】また、上記実施例を記録媒体の発明として把握することができる。つまり、上記実施例は、情報流通システムにおいて、暗号化されている原情報を復号する原情報復号手段と、上記復号された原情報に、情報埋め込み鍵によって利用者認証子を埋め込む利用者認証子埋め込み手段ととしてコンピュータを機能させるためのプログラムを記録したコンピュータ読取可能な記録媒体である。

【0041】

【発明の効果】本発明によれば、情報流通システムにお

いて、利用者が購入した暗号化情報に基づいて、利用者が原情報を不正複製することを阻止することができるという効果を奏する。

【図面の簡単な説明】

【図1】本発明の一実施例である原情報保護装置（外部装置）50を、利用者端末10と情報配送センタ10とともに示すブロック図である。

【図2】原情報保護装置50の具体例を示すブロック図である。

【図3】上記実施例の動作を示すフローチャートである。

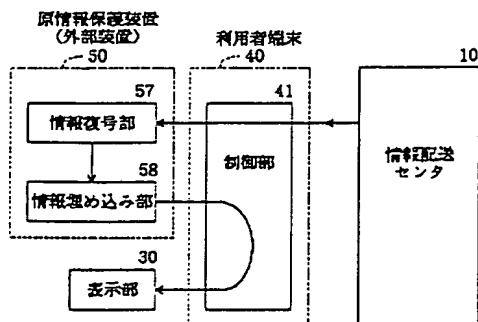
【図4】従来の情報流通システムIFSを示すブロック図である。

【図5】上記従来例の動作を示す図である。

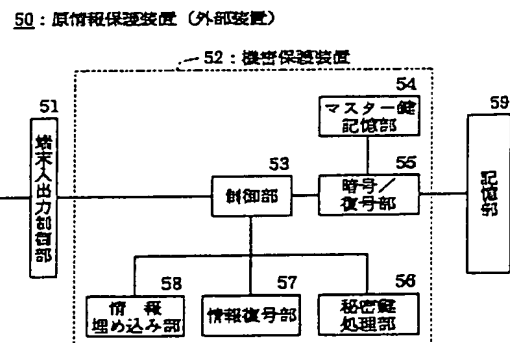
【符号の説明】

- 10…情報配送センタ、
- 30…表示部、
- 40…利用者端末、
- 41…制御部、
- 50…原情報保護装置、
- 51…端末入出力制御部、
- 52…機密保護装置、
- 53…制御部、
- 54…マスター鍵記憶部、
- 55…暗号／復号部、
- 56…秘密鍵処理部、
- 57…情報復号部、
- 58…情報埋め込み部、
- 59…記憶部。

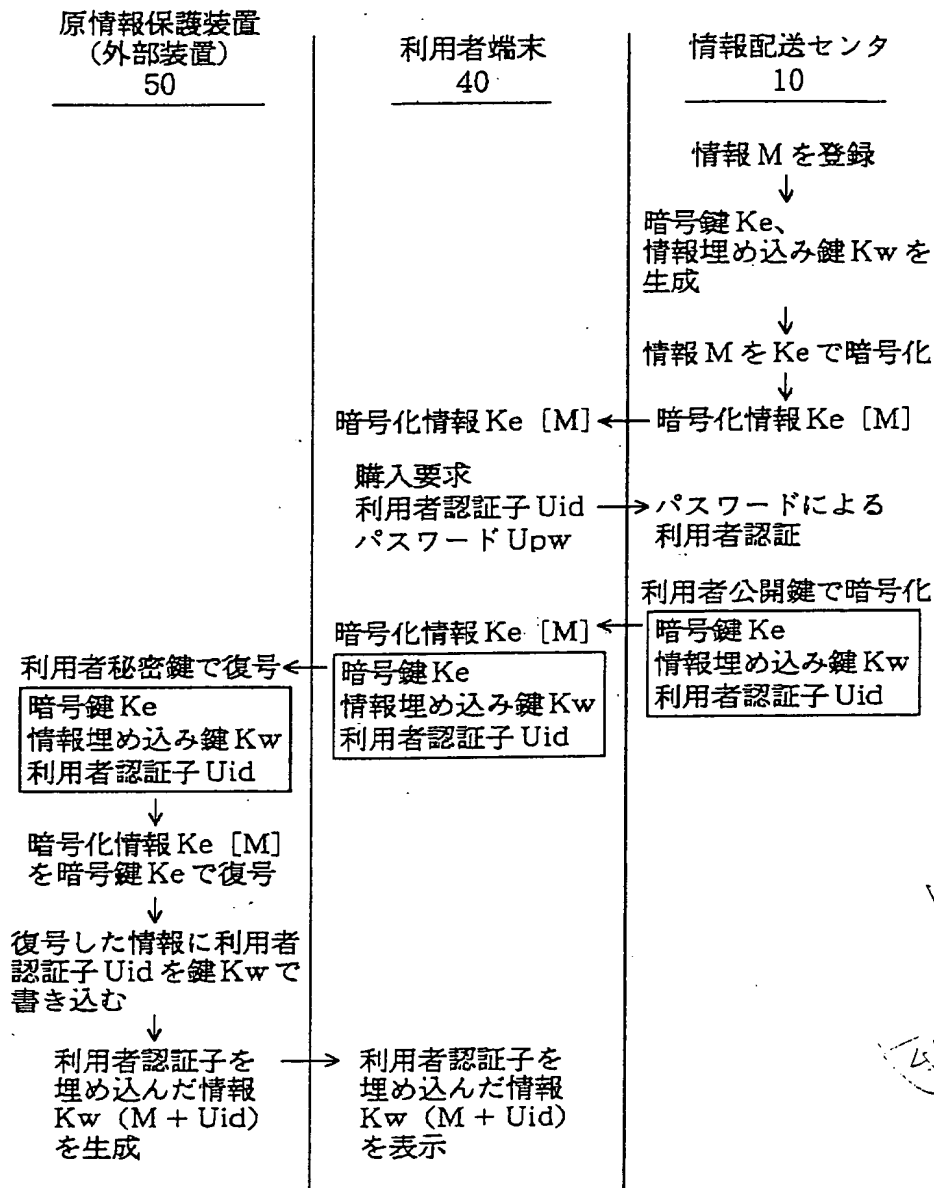
【図1】



【図2】

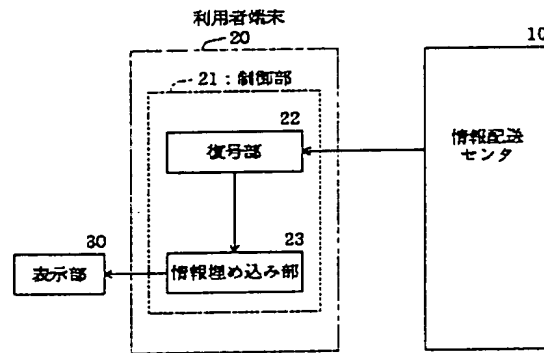


【図 3】

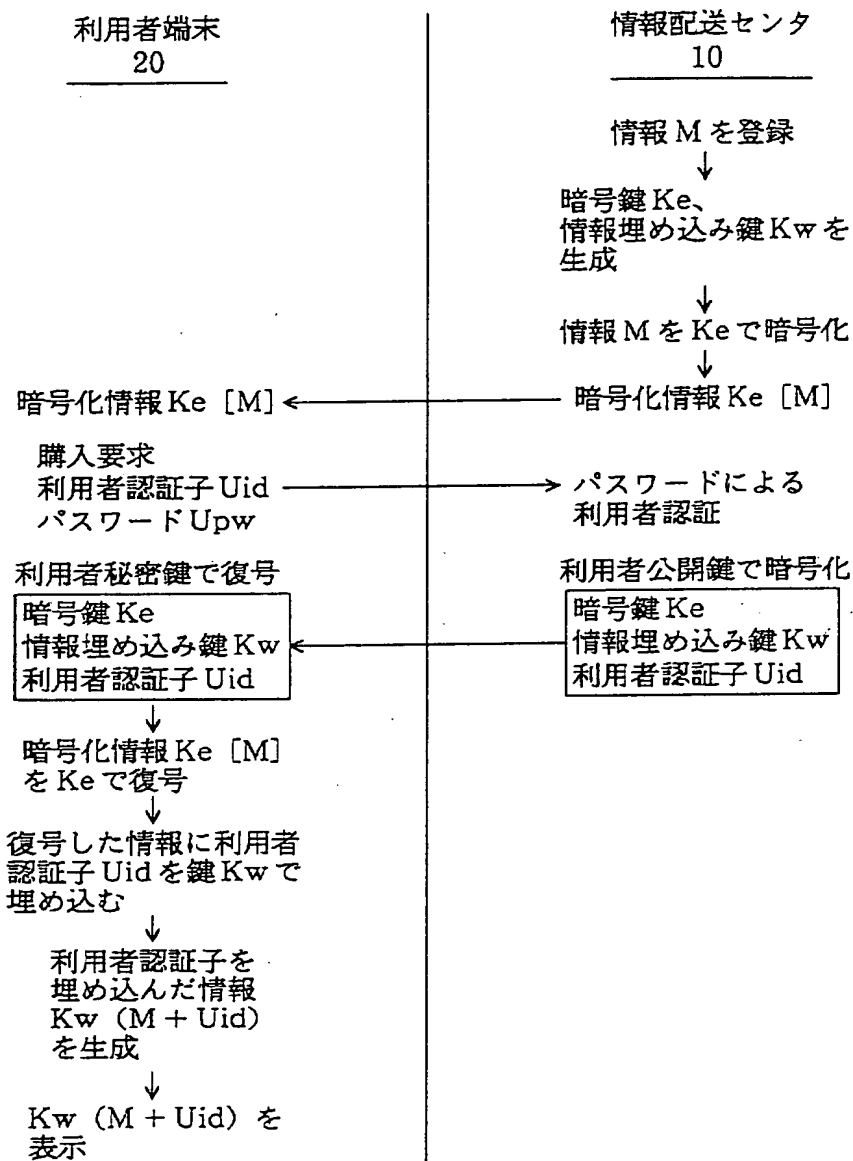


【図 4】

[FS: 従来の情報流通システム]



【図 5】



K4145

フロントページの続き

(51)Int.Cl.⁶

識別記号

F I

H 0 4 L 9/00

6 7 5 D

(72)発明者 河久保 秀二
東京都新宿区西新宿三丁目19番2号 日本
電信電話株式会社内